PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-175600
(43)Date of publication of application : 29.06.2001

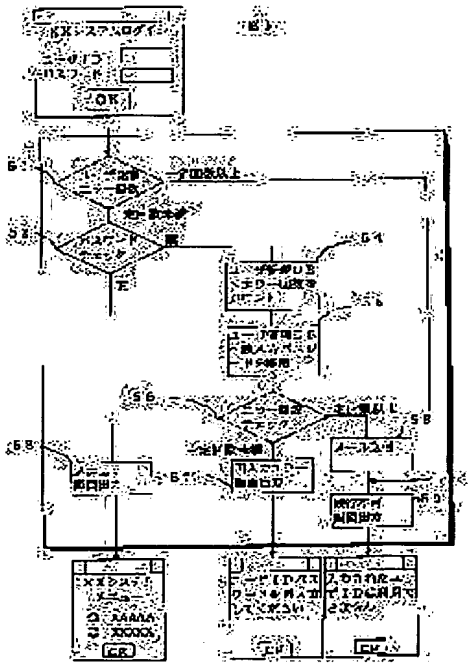
(51)Int.Cl. G06F 15/00
G06F 1/00
G09C 1/00
H04L 9/32

(21)Application number : 11-356544
(22)Date of filing : 15.12.1999

(71)Applicant : HITACHI LTD
(72)Inventor : WADA AKIFUMI

(54) METHOD AND DEVICE FOR REPORTING ILLEGAL ACCESS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for detecting and processing the possibility of illegal access by impersonating in the case of user authentication when a user logs in through the internet to a job application.
SOLUTION: A user authentication application judges whether inputted user ID and password are coincident with a previously registered password or not and when it is judged that the password is not coincident with the registered password, it is judged whether the password is not coincident continuously more than prescribed times or not. When the password is not coincident more than prescribed times, while referring to a mail address registered concerning the relevant user, electronic mail reporting illegal access is transmitted to that mail address.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開２００１－１７５６００

(Ｐ２００１－１７５６００Ａ)

(43)公開日　平成13年6月29日(2001.6.29)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０　Ｂ	5B085
	1/00	３７０		1/00	３７０　Ｅ	5J104
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０　Ｅ	9A001
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３　Ａ	
					６７５　Ｚ	

審査請求　未請求　請求項の数５　ＯＬ　(全７頁)

(21)出願番号　特願平11-356544

(22)出願日　平成11年12月15日(1999.12.15)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72)発明者　和田　暁史
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報システム事業部内

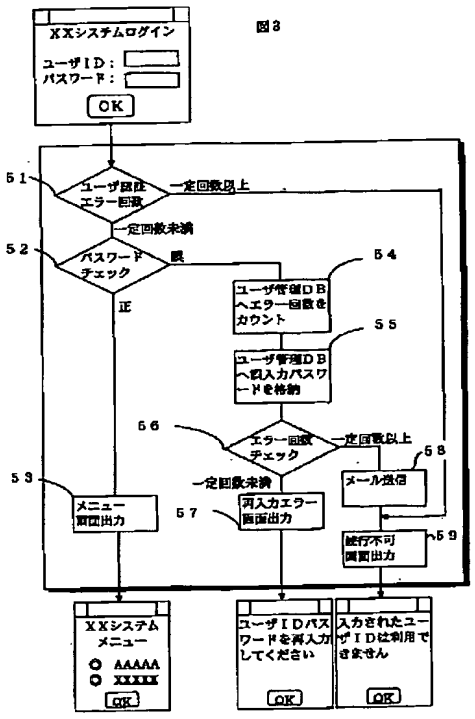
(74)代理人　100068504
弁理士　小川　勝男　(外1名)

Ｆターム(参考)　5B085 AE02 AE03 AE23
5J104 AA07 KA01 NA05 NA27 PA08
9A001 CC07 DD15 EE03 JJ14 JJ25
JJ27 KK56 LL03

(54)【発明の名称】不正アクセス通知方法及びその装置

(57)【要約】
【課題】　ユーザがインターネットを介して業務アプリケーションにログインする際のユーザ認証において、成りすましによる不正アクセスの可能性を検出して処置する方法を提供する。
【解決手段】　ユーザ認証アプリケーションは、投入されたユーザＩＤとパスワードがあらかじめ登録されたパスワードに一致するか否か判定し、そのパスワードが登録されたパスワードに一致しないと判定したとき連続して所定回数以上不一致か否かを判定し、所定回数以上不一致と判定したとき当該ユーザについて登録されたメールアドレスを参照してそのメールアドレス宛てに不正アクセスを通知する電子メールを送信する。

図3



1

【特許請求の範囲】

【請求項１】ユーザＩＤとパスワードによってユーザを認証する方法において、ユーザから投入されたパスワードがあらかじめ登録されたパスワードに一致するか否か判定し、該パスワードが登録されたパスワードに一致しないと判定したとき連続して所定回数以上不一致か否かを判定し、所定回数以上不一致と判定したとき当該ユーザについて登録されたメールアドレスを参照して該メールアドレス宛てに不正アクセスを通知する電子メールを送信することを特徴とする不正アクセス通知方法。

【請求項２】前記電子メールによる通知に、誤入力されたパスワードのリストを添付することを特徴とする請求項１記載の不正アクセス通知方法。

【請求項３】業務アプリケーションを実行する計算機と端末とがインターネットを介して接続されるシステムにおける該計算機による端末ユーザの認証方法において、該端末から投入されたユーザＩＤとパスワードの組があらかじめ登録されたユーザＩＤとパスワードの組に一致するか否か判定し、該パスワードが登録されたパスワードに一致しないと判定したとき連続して所定回数以上不一致か否かを判定し、所定回数以上不一致と判定したとき当該ユーザについて登録されたメールアドレスを参照して該メールアドレス宛てに不正アクセスを通知する電子メールを送信することを特徴とする不正アクセス通知方法。

【請求項４】コンピュータ読み取り可能なプログラムを格納する記憶媒体であり、該プログラムはユーザＩＤとパスワードによってユーザを認証するプログラムであって、該プログラムは下記機能を含むことを特徴とするプログラムを格納する記憶媒体：ユーザから投入されたパスワードがあらかじめ登録されたパスワードに一致するか否か判定する機能、該パスワードが登録されたパスワードに一致しないと判定したとき連続して所定回数以上不一致か否かを判定する機能、および所定回数以上不一致と判定したとき当該ユーザについて登録された宛先宛てに不正アクセスを通知する機能。

【請求項５】インターネットに接続され、ユーザＩＤとパスワードによってユーザを認証するサーバマシンにおいて、該サーバマシンは、各ユーザに対応してユーザＩＤ、パスワード及びメールアドレスを登録するデータベースと、ユーザから投入されたユーザＩＤとパスワードの組が該データベースに登録されたユーザＩＤとパスワードの組に一致するか否か判定する手段と、該パスワードが登録されたパスワードに一致しないと判定したとき連続して所定回数以上不一致か否かを判定する手段と、所定回数以上不一致と判定したとき当該ユーザについて登録されたメールアドレスを参照して該メールアドレス宛てに不正アクセスを通知する電子メールを送信する手段とを有することを特徴とする不正アクセスを通知するサーバマシン。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザを認証する方法に係わり、特に業務システムへのログイン時に正当なユーザに対する成りすましの不正アクセスを検出して正当なユーザに通知する方法に関する。

【０００２】

【従来の技術】ユーザがインターネットのような広域ネットワークを介して業務アプリケーションを実行するサーバマシンにアクセスするとき、サーバマシンはその業務システムへのユーザのログイン時にアクセス者が正当な業務利用者か否かチェックする必要がある。この種の業務システムは、業務利用者の業務システムへのログイン時に端末装置にユーザ認証画面を表示させ、業務利用者がその画面を介して入力したユーザＩＤとパスワードが正当な業務利用者のユーザＩＤとパスワードかどうかチェックする。不正なパスワードが入力されると、ユーザ認証エラーが発生し、エラー発生回数が一定回数を越えた場合、業務システムへのログインを不可能にすることによって不正アクセスを防止する。

【０００３】

【発明が解決しようとする課題】従来の不正アクセス防止方法によると、正当な業務利用者がログインを試みてログイン不可能となった場合に、自分のユーザＩＤが他人に不正に利用されたか、あるいはその他の原因によるエラー発生なのか分からないという問題がある。特にインターネットを利用する業務システムにおいては、このような問題の発生する可能性が非常に大きいと考えられる。

【０００４】本発明の目的は、他人によるユーザＩＤの不正利用を検出して処置する方法を提供することにある。

【０００５】

【課題を解決するための手段】本発明は、ユーザから投入されたパスワードがあらかじめ登録されたパスワードに一致するか否か判定し、そのパスワードが登録されたパスワードに一致しないと判定したとき連続して所定回数以上不一致か否かを判定し、所定回数以上不一致と判定したとき当該ユーザについて登録されたメールアドレスを参照してそのメールアドレス宛てに不正アクセスを通知する電子メールを送信する不正アクセス通知方法及び装置を特徴とする。

【０００６】

【発明の実施の形態】以下、本発明の実施形態について図面を用いて詳細に説明する。

【０００７】図１は、本実施形態によるインターネットを利用する業務システムの構成図である。図１において、１０は業務アプリケーションを搭載するサーバマシン、２０は業務システム利用者が利用する端末、３０はサーバマシン１０と端末２０とを接続するインターネッ

トである。本実施形態では端末２０は１台しか示されていないが、複数台の端末２０をサーバマシン１０に接続可能である。このシステムにおいて端末２０がサーバマシン１０にログインする際にユーザ認証を必要とする。

【０００８】サーバマシン１０は、ユーザ認証アプリケーション１２とユーザ管理ＤＢ（データベース）１１を有し、端末２０の表示装置は、業務利用者がユーザＩＤとパスワードを入力するためのユーザ認証画面２１を表示する。業務利用者がユーザ認証画面２１を介して入力したユーザＩＤとパスワードは、インターネット３０を介してサーバマシン１０へ送られ、そのユーザ認証アプリケーション１２が受信する。ユーザ認証アプリケーション１２は、ユーザ管理ＤＢ１１を参照し、ユーザＩＤとパスワードをチェックすることによってユーザ認証を行う。

【０００９】ユーザ認証アプリケーション１２のプログラムを記憶媒体に格納し、サーバマシン１０に接続される駆動装置を介してサーバマシン１０のメモリに読み込むか、または他の計算機に接続される駆動装置、他の計算機及びネットワークを介してサーバマシン１０に伝送し、サーバマシン１０によって実行することが可能である。

【００１０】次にユーザ管理ＤＢ１１の構成について図２に従って説明する。図２は、ユーザ管理ＤＢ１１内の管理データの内容を示したものである。ユーザ管理ＤＢ１１の各レコードは、各業務利用者に対応してユーザＩＤ４１、パスワード４２、メールＩＤ４３、エラー発生回数４４及び誤入力パスワード４５を格納する。ユーザＩＤ４１及びパスワード４２はその業務利用者に対して発行されたユーザＩＤとパスワード、メールＩＤ４３は業務利用者の電子メールアドレスである。エラー発生回数４４はパスワードの入力誤りの発生した回数であり、誤入力パスワード４５は誤入力されたパスワードのリストである。

【００１１】次にユーザ認証アプリケーション１２のユーザ認証処理手順について、図３のフローチャートに従って説明する。ユーザ認証アプリケーション１２は、端末に表示されたユーザ認証画面２１を介して業務利用者によって入力されたユーザＩＤとパスワードを受信すると、受信したユーザＩＤをもとにユーザ管理ＤＢ１１のエラー発生回数４４のエリアを参照してユーザ認証エラー発生回数をチェックし（ステップ５１）、一定回数以上の場合には続行不可能画面を表示する（ステップ５９）。一定回数未満の場合には、受信したユーザＩＤをもとにユーザ管理ＤＢ１１から該当する業務利用者のパスワードを検索し、正当な業務利用者か否かのチェックを行う（ステップ５２）。正当な業務利用者であれば、業務システムメニュー画面を表示する（ステップ５３）。パスワードの一致しない業務利用者の場合には、ユーザ管理ＤＢ１１のユーザ認証に関するエラー発生回数４４のエリアにエラー回数を格納する（ステップ５４）。またユーザ管理ＤＢ１１の誤入力パスワード４５のエリアに、受信した誤入力パスワードを格納する（ステップ５５）。その後、ユーザ管理ＤＢ１１のエラー発生回数４４をチェックする（ステップ５６）。一定回数未満であれば、再入力エラー画面を表示する（ステップ５７）。一定回数以上の場合には、該当する業務利用者に対し、ユーザＩＤが他人によって不正に利用されている可能性があることを連絡する電子メールを送信し（ステップ５８）、業務続行不可能画面を表示する（ステップ５９）。

【００１２】ステップ５１でエラー発生回数４４が一定回数以上の場合には、過去に正当な利用者にメール送信の通知をしているので、単に業務続行不可の処理をするだけである。正当な利用者へのメールには、ユーザＩＤが他人によって不正に利用されている可能性がある旨の通知とともに、その利用者の誤入力パスワード４５を添付する。正当な利用者は、このメールを受信したとき、添付された誤入力パスワード４５をみてユーザＩＤが不正に使用されているかどうかを判定することができる。ユーザＩＤが不正に使用されている場合には、メールをシステム管理者に提示し、ユーザＩＤとパスワードを変更することが可能である。

【００１３】なおユーザ認証画面２１を介するユーザＩＤとパスワードの入力は、業務利用者の手入力であってもよいし、業務利用者所有のＩＣカードからの入力であっても構わない。

【００１４】またメール送信については、サーバマシン１０にメール送信プログラムを搭載し、ユーザ認証アプリケーション１２からリアルタイムにメール送信を要求するコマンドを発行してもよいし、業務終了後にバッチ処理によってユーザ管理ＤＢ１１のエラー発生回数４４を参照しユーザ認証エラー発生回数が一定回数以上のユーザについてメール送信プログラムを介してメール送信してもよい。バッチ処理の場合には、メール送信済みのレコードにフラグを立て、１回だけのメール送信とする。なお誤入力パスワード４５とともに不正にアクセスした端末２０のＩＰアドレスなどを記録しておけば、不正アクセスした端末を追跡することができる。

【００１５】また図４のステップ６１のように、パスワードチェックでＯＫとなったタイミングでユーザ管理ＤＢ１１のエラー発生回数４４を０クリアしてもよい。またエラー発生回数４４が一定回数を越えた場合に、正当な業務利用者について新しいユーザＩＤを再登録してもよい。０クリアするタイミングもパスワードチェックでＯＫとなったタイミングではなく、１日単位で０クリアしてもよい。

【００１６】

【発明の効果】以上説明したように本発明によれば、ユーザ認証の際のエラー発生回数が所定回数以上になった

とき、正当な業務利用者に対して不正アクセスの可能性があることを通知するので、業務利用者は、他人の成りすましによる不正アクセスかそれ以外の原因によるエラー発生かを切り分け、それに応じて対策することができる。

【図面の簡単な説明】

【図１】実施形態のシステムの構成図である。

【図２】実施形態のユーザ管理ＤＢの構成を示す図である。

【図３】実施形態のユーザ認証処理手順を示すフローチャートである。

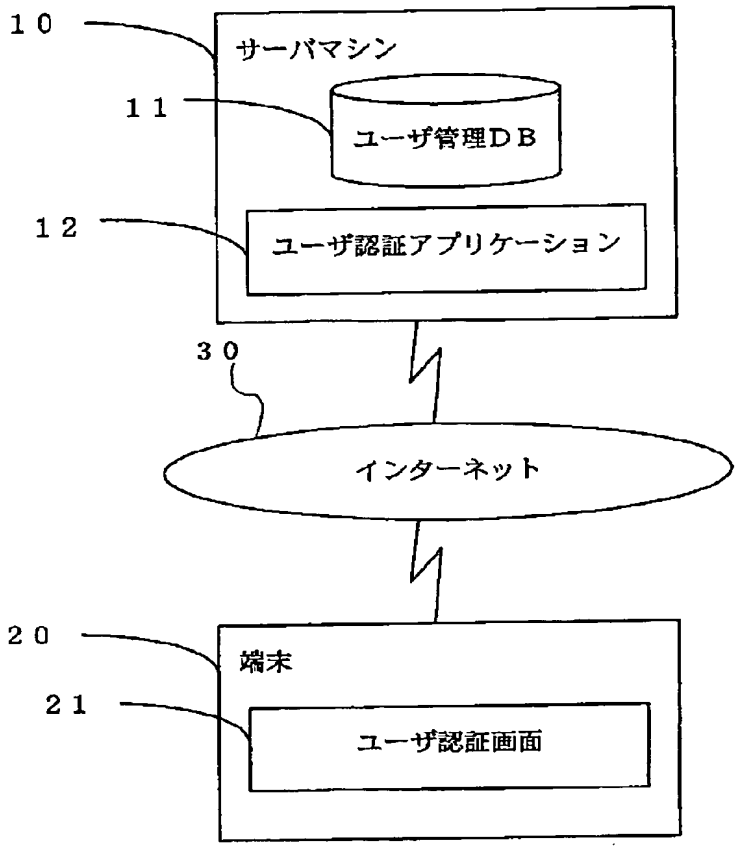
【図４】他の実施形態のユーザ認証処理手順を示すフローチャートである。

【符号の説明】

１０：サーバマシン、１１：ユーザ管理ＤＢ、１２：ユーザ認証アプリケーション、２０：端末、３０：インターネット、４１：ユーザＩＤ、４２：パスワード、４３：メールＩＤ、４４：エラー発生回数、４５：誤入力パスワード

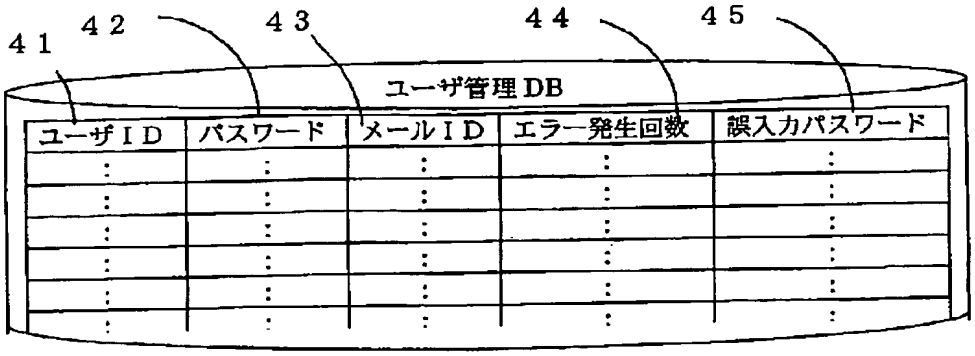
【図１】

図１

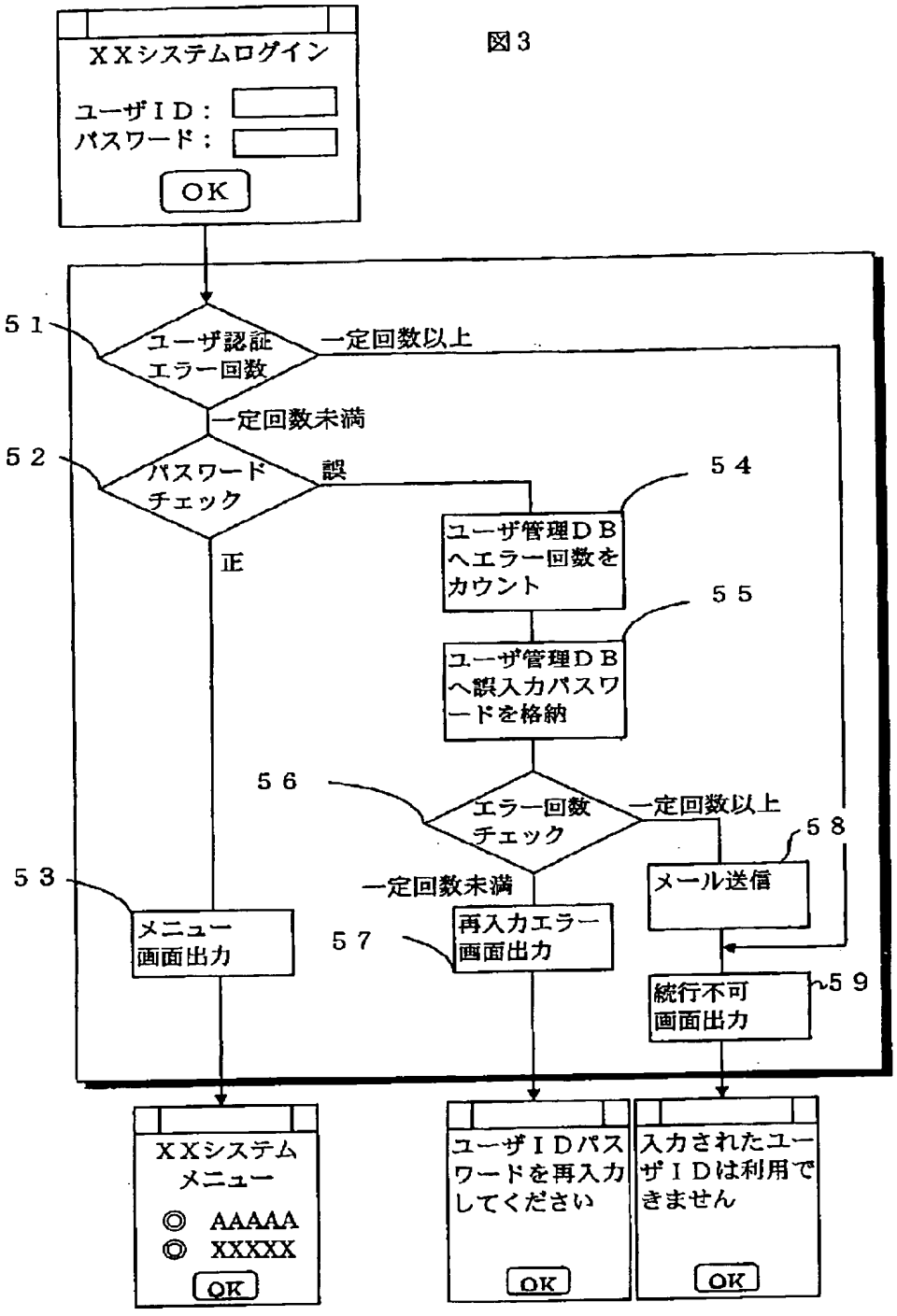


【図２】

図２

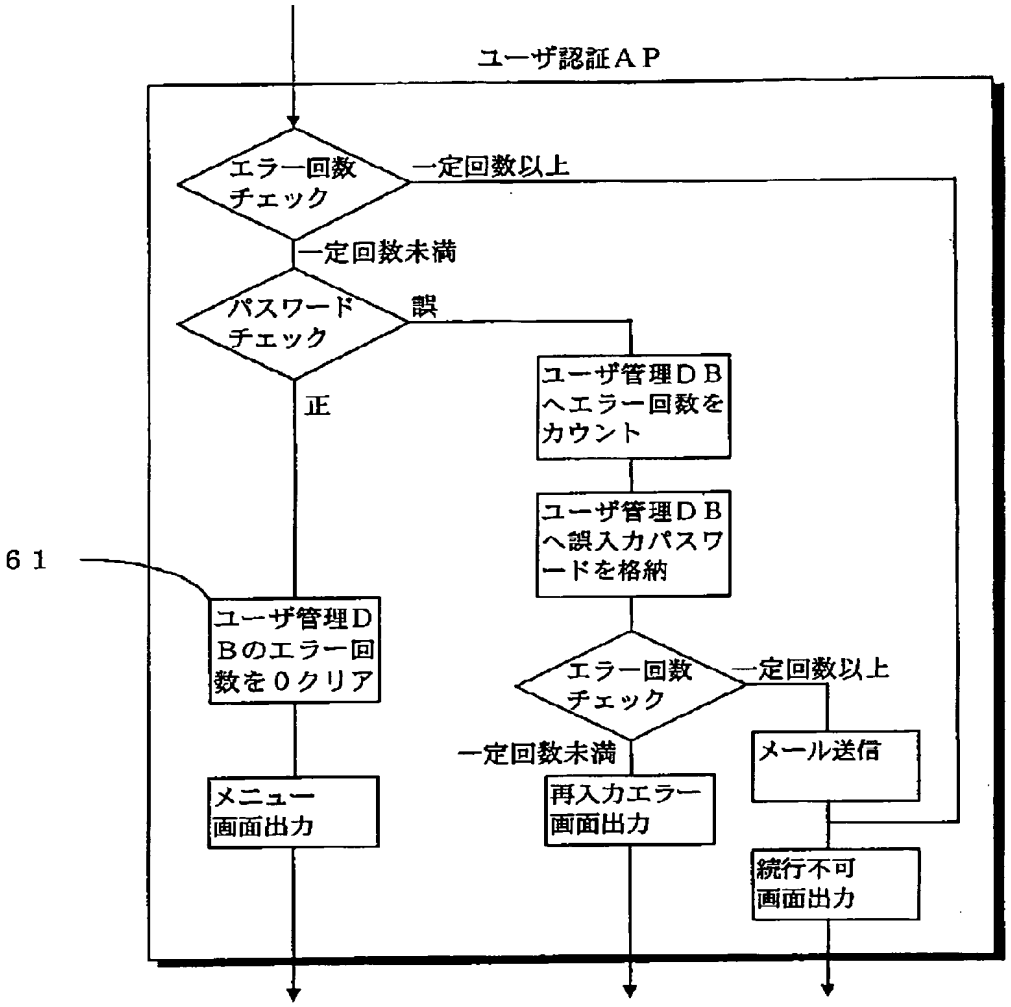


【図３】


ＸＸシステムログイン
ユーザＩＤ：
パスワード：
ＯＫ
図３
５１
ユーザ認証
エラー回数
一定回数以上
一定回数未満
５２
パスワード
チェック
誤
正
５４
ユーザ管理ＤＢ
へエラー回数を
カウント
５５
ユーザ管理ＤＢ
へ誤入力パスワ
ードを格納
５６
エラー回数
チェック
一定回数以上
一定回数未満
５８
メール送信
５３
メニュー
画面出力
５７
再入力エラー
画面出力
５９
続行不可
画面出力
ＸＸシステム
メニュー
◎ AAAAA
◎ XXXXX
ＯＫ
ユーザＩＤパス
ワードを再入力
してください
ＯＫ
入力されたユー
ザＩＤは利用で
きません
ＯＫ

【図４】

図４


ユーザ認証ＡＰ
エラー回数チェック
一定回数以上
一定回数未満
パスワードチェック
誤
正
ユーザ管理ＤＢへエラー回数をカウント
ユーザ管理ＤＢへ誤入力パスワードを格納
61
ユーザ管理ＤＢのエラー回数を０クリア
エラー回数チェック
一定回数以上
一定回数未満
メール送信
メニュー画面出力
再入力エラー画面出力
続行不可画面出力